IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application. An identifier indicating the status of each claim is provided.

Listing of Claims

1 – 68. (Canceled)

69.   (Currently Amended) An information distribution system for distributing ~~predetermined~~ data from an information sending device to an information receiving device, ~~characterized in that~~ wherein said information sending device comprises:

sending means for sending a plurality of distribution keys, each corresponding to a predetermined time period, and send data, ~~including said~~ which includes data encrypted with key data; ~~for distribution given in advance,~~ and

said information receiving device comprises:

receiving means for receiving said send data and said plurality of distribution keys; and

receiving end controlling means for decrypting said encrypted data, ~~using said key data given in advance.~~

wherein each of said plurality of distribution keys allows decryption of said encrypted data within the predetermined time period associated with said distribution key, independent of a connection during said predetermined time period associated with said distribution key.

70.   (Currently Amended) An information distribution method for distributing predetermined data from an information sending device to an information receiving device, ~~characterized by~~ ~~comprising:~~

BEST AVAILABLE COPY

wherein said method comprises:

a sending step ~~of~~ for sending _a plurality of distribution keys, each corresponding to a predetermined time period, and_ send data ~~including~~ which includes ~~said~~ data encrypted with key data ~~for distribution given in advance, by said information sending device~~; and

a decrypting step ~~of~~ for receiving said send data _and said plurality of distribution keys;_ ~~, and~~ decrypting said encrypted data; and

permitting decryption of said encrypted data within the predetermined time period associated with said distribution key, independent of a connection during said predetermined time period associated with said distribution key.

~~using said key data given in advance, by said information receiving device.~~

71.   (Currently Amended) An information sending device for sending predetermined data to an information receiving device, ~~characterized by comprising:~~ said device comprising:

sending end controlling means for generating _a plurality of distribution keys, each corresponding to a predetermined time period, and_ send data ~~including said~~ which includes data encrypted using key data; and ~~for distribution given in advance to said information receiving device; and~~

sending means for sending said send data _and said plurality of distribution keys,_

wherein each of said plurality of distribution keys allows decryption of said encrypted data within the predetermined time period associated with said distribution key, independent of a connection during said predetermined time period associated with said distribution key.

-4-

00265507

72.   (Original) The information sending device according to Claim 71, characterized in that

said sending end controlling means generates send data including an individual key

specific to said information sending device, as said data encrypted with said key data.

73.   (Original) The information sending device according to Claim 72, characterized in that

said sending end controlling means generates send data including said data encrypted

using said key data that is periodically updated.

74.   (Original) The information sending device according to Claim 73, characterized in that

said sending end controlling means generates said send data including said encrypted data

using said key data appropriate to an update period, in said data encrypted using said key data for

a plurality of update periods given in advance together.

75.   (Currently Amended) An information receiving device for receiving predetermined data

sent from an information sending device, ~~characterized by comprising:~~ said device comprising:

receiving means for receiving a plurality of distribution keys, each corresponding to a

predetermined time period, and send data ~~including said~~which includes data encrypted with key

data for distribution; and ~~, sent from said information sending device; and~~

receiving end controlling means for decrypting said encrypted data, ~~using said key data~~

~~given in advance.~~

wherein each of said plurality of distribution keys allows decryption of said encrypted

data within the predetermined time period associated with said distribution key, independent of a

connection during said predetermined time period associated with said distribution key.

-5-

00265507

76.   (Original) The information receiving device according to Claim 75, characterized in that

said receiving means receives send data including an individual key specific to said

information receiving device, as said data encrypted with said key data.

77.   (Original) The information receiving device according to Claim 76, characterized in that

said receiving means receives said send data including said data encrypted with said key

data that is periodically updated, and

said receiving end controlling means decrypts said data using said key data that is

periodically updated and given.

78.   (Original) The information receiving device according to Claim 77, characterized in that

said receiving end controlling means decrypts said data using said key data appropriate to

an update period, in said key data for plurality of update periods given in advance.

79.   (Currently Amended) An information sending method for sending predetermined data to

an information receiving device, ~~characterized by comprising~~

wherein said method comprises:

a generating step of generating a plurality of distribution keys, each corresponding to a

predetermined time period, and send data ~~including said~~which includes data encrypted using key

~~data for distribution given in advance to said information receiving device~~; and

a sending step of sending said send data and said plurality of distribution keys.

-6-

wherein each of said plurality of distribution keys allows decryption of said encrypted data within the predetermined time period associated with said distribution key, independent of a connection during said predetermined time period associated with said distribution key.

80.   (Original) The information sending method according to Claim 79, characterized in that in said generating step, send data including an individual key specific to said information sending device is generated as said data encrypted with said key data.

81.   (Original) The information sending method according to Claim 80, characterized in that in said generating step, send data including said data encrypted using said key data that is updated periodically is generated.

82.   (Original) The information sending method according to Claim 81, characterized in that in said generating step, said send data including said data encrypted using said key data appropriate to an update period, it said data encrypted using said key data for a plurality of update periods given together in advance, is generated.

83.   (Currently Amended) An information receiving method for receiving predetermined data sent from an information sending device, ~~characterized by comprising~~

wherein said method comprises:

a receiving step of receiving a plurality of distribution keys, each corresponding to a predetermined time period, and send data ~~including said~~which includes data encrypted with key data for distribution, ~~sent from said information sending device~~; ~~and~~

-7-

a decrypting step of decrypting said ~~encrypted data; and~~ using said key data given in ~~advance~~

allowing decryption of said encrypted data within the predetermined time period associated with said distribution key, independent of a connection during said predetermined time period associated with said distribution key.

84.   (Original) The information receiving method according to Claim 83, characterized in that in said receiving step, send data including an individual key specific to said information receiving device is received as said data encrypted with said key data.

85.   (Original) The information receiving method according to Claim 84, characterized in that in said receiving step, said send data including said data encrypted with said key data that is updated periodically is received, and

in said decrypting step, said data is decrypted using said key data that is periodically updated and given.

86.   (Original) The information receiving method according to Claim 85, characterized in that in said decrypting step, said data is decrypted using said key data appropriate to an update period, in said key data for a plurality of update periods given together in advance.

87.   (Currently Amended) A program storing medium for making an information sending device run a program, ~~characterized by comprising~~

wherein said method comprises:

-8-   00265507

a generating step of generating <u>a plurality of distribution keys, each corresponding to a</u> <u>predetermined time period, and</u> send data ~~including predetermined~~<u>which includes</u> data encrypted using key data ~~for distribution given in advance to an information receiving device~~; ~~and~~

a sending step of sending said send data <u>and said plurality of distribution keys</u> to said information receiving device<u>; and</u>

<u>allowing decryption of said encrypted data within the predetermined time period</u> <u>associated with said distribution key, independent of a connection during said predetermined</u> <u>time period associated with said distribution key.</u>

88.   (Original) The program storing medium according to Claim 87, characterized in that

in said generating step, send data including an individual key specific to said information sending device is generated as said data encrypted with said key data.

89.   (Original) The program storing medium according to Claim 88, characterized in that

in said generating step, send data including said data encrypted using said key data that is updated periodically is generated.

90.   (Original) The program storing medium according to Claim 89, characterized in that

in said generating step, said send data including said data encrypted using said key data appropriate to an update period, in said data encrypted using said key data for a plurality of update periods given together in advance is generated.

-9-

00265507

91.   (Currently Amended) A program storing medium for making an information receiving

device run a program, ~~characterized by comprising~~

wherein said program comprises:

a receiving step of receiving a plurality of distribution keys, each corresponding to a

predetermined time period, and send data ~~including predetermined~~ which includes data encrypted

with key data ~~for distribution, sent from an information sending device;~~ ~~and~~

a decrypting step of decrypting said encrypted data; and ~~using said key data given in~~

~~advance~~

allowing decryption of said encrypted data within the predetermined time period

associated with said distribution key, independent of a connection during said predetermined

time period associated with said distribution key.

92.   (Original) The program storing medium according to Claim 91, characterized in that

in said receiving step, send data including an individual key specific to said information

receiving device is received as said data encrypted with said key data.

93.   (Original) The program storing medium according to Claim 92, characterized in that

in said receiving step, said send data including said data encrypted with said key data that

is updated periodically is received, and

in said decrypting step, said data is decrypted using said key data that is periodically

updated and given.

94.   (Original) The program storing medium according to Claim 93, characterized in that

-10-

00265507

in said decrypting step, said data is decrypted using said key data appropriate to an update

period, in said key data for plurality of update periods given together in advance.

95.   (Currently Amended) An information distribution system for distributing predetermined

content data from an information sending device to an information receiving device,

~~characterized in that~~

said information sending device comprises:

sending end controlling means for encrypting said content data with a content key, and

encrypting the content key with an individual key specific to said information sending device;

and

sending means for sending an encrypted individual key ~~mage~~ by encrypting said

individual key with <u>one of</u> a <u>plurality of distribution keys, each distribution key corresponding to</u>

<u>a predetermined time period</u> ~~predetermined distribution key, which is supplied from the outside~~,

to said information receiving device together with said content data encrypted with said content

key and a content key encrypted with said individual key, and

said information receiving device comprises:

receiving means for receiving said content data encrypted with said content key and said

content key encrypted with said individual key together with said encrypted individual key; and

receiving end controlling means for decrypting said individual key with <u>one of said</u>

<u>plurality of distribution keys</u> ~~said distribution key given in advance~~, decrypting said content key

with the decrypted individual key, and decrypting said content data with the decrypted content

key; <u>and</u>

-11-

00265507

PATENT
450108-02659

allowing decryption of said individual key within the predetermined time period associated with said distribution key, independent of a connection during said predetermined time period associated with said distribution key.

96.   (Currently Amended) An information distribution method for distributing predetermined content data from an information sending device to an information receiving device, ~~characterized by comprising~~wherein said method comprises:

a sending step of encrypting said content data with a content key, encrypting the content key with an individual key specific to said information sending device, and sending an encrypted individual key made by encrypting said individual key with one of a plurality of distribution keys, each distribution key corresponding to a predetermined time period~~a predetermined distribution key, which is supplied from the outside~~, to said information receiving device together with said content data encrypted with said content key and a content key encrypted with said individual key, by said information sending device; ~~and~~

a decrypting step of receiving said content data encrypted with said content key and said content key encrypted with said individual key together with said encrypted individual key, decrypting said individual key with one of said plurality of distribution keys ~~said distribution key given in advance~~, decrypting said content key with the decrypted individual key, and decrypting said content data with the decrypted content key, by said information receiving device; and

allowing decryption of said individual key within the predetermined time period associated with said distribution key, independent of a connection during said predetermined time period associated with said distribution key.

-12-

97.   (Currently Amended) An information sending device for sending predetermined content data to an information receiving device, ~~characterized by~~ said device comprising:

sending end controlling means for encrypting said content data with a content key, and encrypting the content key with an individual key specific to said information sending device; ~~and~~

sending means for sending an encrypted individual key made by encrypting said individual key with one of a plurality of distribution keys, each distribution key corresponding to a predetermined time period ~~a predetermined distribution key, which is supplied from the outside~~, to said information receiving means together with said content data encrypted with said content key and said content key encrypted with said individual key; and

allowing decryption of said individual key within the predetermined time period associated with said distribution key, independent of a connection during said predetermined time period associated with said distribution key.

98.   (Original) The information sending device according to Claim 97, characterized in that said sending end controlling means encrypts said content key with said individual key supplied from the outside together with said encrypted individual key.

99.   (Original) The information sending device according to Claim 98, characterized in that said sending means sends said encrypted individual key made by encrypting said individual key with said distribution key that is updated periodically, which is supplied from the outside, to said information receiving device together with said content data encrypted with said content key and said content key encrypted with said individual key.

-13-   00265507

100.   (Original) The information sending device according to Claim 99, characterized in that

said sending means sends said encrypted individual key appropriate to an update period,

in said encrypted individual key for a plurality of periods given together in advance to said

information receiving device together with said content data encrypted with said content key and

a content key encrypted with said individual key.

101.   (Currently Amended) An information receiving device for receiving predetermined

content data sent from an information sending device, ~~characterized by~~ said device comprising:

receiving means for receiving said content data encrypted with a content key, said content

key encrypted with an individual key specific to said information sending device, and said

individual key encrypted with <u>one of a plurality of distribution keys, each distribution key</u>

<u>corresponding to a predetermined time period</u> ~~a predetermined distribution key, sent from said~~

~~information sending device;~~ ~~and~~

receiving end controlling means for decrypting said individual key with <u>one of said</u>

<u>plurality of distribution keys</u> ~~said distribution key given in advance~~, decrypting said content key

with the decrypted individual key, and decrypting said content data with the decrypted content

key<u>; and</u>

<u>allowing decryption of said individual key within the predetermined time period</u>

<u>associated with said distribution key, independent of a connection during said predetermined</u>

<u>time period associated with said distribution key.</u>

-14-

102.   (Original) The information receiving device according to Claim 101, characterized in that said receiving end controlling means decrypts said individual key with said distribution key that is updated periodically.

103.   (Original) The information receiving device according to Claim 102, characterized in that said receiving end controlling means decrypts said individual key with said distribution key appropriate to an update period, in said distribution key for a plurality of periods given together in advance.

104.   (Currently Amended) An information sending method for sending predetermined content data to an information receiving device, ~~characterized by comprising:~~ wherein said method comprises:

a encrypting step of encrypting said content data with a content key, and encrypting the content key with an individual key specific to said information sending device; ~~and~~

a sending step of sending an encrypted individual key made by encrypting said individual key with one of a plurality of distribution keys, each distribution key corresponding to a predetermined time period ~~predetermined distribution key, which is supplied from the outside,~~ to said information receiving device together with said content data encrypted with said content key and said content key encrypted with said individual key; and

allowing decryption of said individual key within the predetermined time period associated with said distribution key, independent of a connection during said predetermined time period associated with said distribution key.

-15-

00265507

105.   (Original) The information sending method according to Claim 104, characterized in that in said encrypting step, said content key is encrypted with said individual key supplied from the outside together with said encrypted individual key.

106.   (Original) The information sending method according to Claim 105, characterized in that in said sending step, said encrypted individual key made by encrypting said individual key with said distribution key that is updated periodically, which is supplied from the outside, is sent to said information receiving device together with said content data encrypted with said content key and a content key encrypted with said individual key.

107.   (Original) The information sending method according to Claim 106, characterized in that in said sending step, said encrypted individual key appropriate to an update period, in said encrypted individual key for a plurality of update periods given together in advance, is sent to said information receiving device together with said content data encrypted with said content key and a content key encrypted with said individual key.

108.   (Currently Amended) An information receiving method for receiving predetermined content data sent from an information sending device, ~~characterized by comprising~~ wherein said method comprises:
        a receiving step of receiving said content data encrypted with a content key, said content key encrypted with an individual key specific to said information sending device, and said individual key encrypted with <u>one of a plurality of distribution keys, each distribution key</u>

-16-

corresponding to a predetermined time period ~~a predetermined distribution key, sent from said~~ ~~information sending device~~; and

a decrypting step of decrypting said individual key encrypted with ~~said distribution key~~ ~~given in advance~~ one of said plurality of distribution keys, decrypting said content key with the decrypted individual key, and decrypting said content data with the decrypted content key; and allowing decryption of said individual key within the predetermined time period associated with said distribution key, independent of a connection during said predetermined time period associated with said distribution key.

109.   (Original) The information receiving method according to Claim 108, characterized in that in said decrypting step, said individual key is decrypted with said distribution key that is updated periodically.

110.   (Original) The information receiving method according to Claim 109, characterized in that in said decrypting step, said individual key is decrypted with said distribution key appropriate to an update period, in said distribution key for a plurality of update periods given together in advance.

111.   (Currently Amended) A program storing medium for making an information sending device run a program, said program storing medium ~~, characterized by~~ comprising:

an encrypting step of encrypting predetermined content data with a content key, and encrypting the content key with an individual key specific to an information sending device; ~~and~~

-17-

00265507

a sending step of sending an encrypted individual key made by encrypting said individual key with one of a plurality of distribution keys, each distribution key corresponding to a predetermined time period a predetermined distribution key, which is supplied from the outside, to said information receiving device together with said content data encrypted with said content key and a content key encrypted with said individual key; and

allowing decryption of said individual key within the predetermined time period associated with said distribution key, independent of a connection during said predetermined time period associated with said distribution key.

112.   (Original) The program storing medium according to Claim 111, characterized in that in said encrypting step, said content key is encrypted with said individual key supplied from the outside together with said encrypted individual key.

113.   (Original) The program storing medium according to Claim 112, characterized in that in said sending step, said encrypted individual key made by encrypting said individual key with said distribution key that is updated periodically, which is supplied from the outside, is sent to said information receiving device together with said content data encrypted with said content key and a content key encrypted with said individual key.

114.   (Original) The program storing medium according to Claim 113, characterized in that in said sending step, said encrypted individual key appropriate to an update period, in said encrypted individual key for a plurality of update periods given together in advance, is sent to

-18-

00265507

said information receiving device together with said content data encrypted with said content key and a content key encrypted with said individual key.

115.   (Currently Amended) A program storing medium for making an information receiving device run a program, ~~characterized by~~ said program storing medium comprising:

a receiving step of receiving predetermined content data encrypted with a content key, said content key encrypted with an individual key specific to said information sending device, and said individual key encrypted with one of a plurality of distribution keys, each distribution key corresponding to a predetermined time period ~~a predetermined distribution key, sent from an information sending device~~; and

a decrypting step of decrypting said individual key with one of said plurality of distribution keys ~~said distribution key given in advance~~, decrypting said content key with the decrypted individual key, and decrypting said content data with the decrypted content key, wherein each of said plurality of distribution keys allows decryption of said individual key within the predetermined time period associated with said distribution key, independent of a connection during said predetermined time period associated with said distribution key.

116.   (Original) The program storing medium according to Claim 115, characterized in that in said decrypting step, said individual key is decrypted with said distribution key that is updated periodically.

-19-

00265507

117.   (Original) The program storing medium according to Claim 116, characterized in that in said decrypting step, said individual key is decrypted with said distribution key appropriate to an update period, in said distribution key for a plurality of update periods given together in advance.

118 – 147. (Canceled)

148.   (Currently Amended) An information distribution system for sending content data encrypted with a predetermined content key from an information sending device to an information receiving device, ~~characterized in that~~

said information sending device comprises:

sending end controlling means for encrypting said content key with an individual key specific to said information sending device; and

sending means for sending at least said content key encrypted with said individual key, and an encrypted individual key made by encrypting said individual key with <u>one of a plurality of distribution keys, each distribution key corresponding to a predetermined time period</u> ~~an distribution key that is updated in a predetermined cycle, which is supplied from the outside~~, to said information receiving device, and

said information receiving device comprises:

receiving means for receiving at least said content key encrypted with said individual key and said encrypted individual key; and

receiving end controlling means for decrypting said individual key with <u>one of said plurality of distribution keys</u> ~~said distribution key given in advance~~, decrypting said content key with the decrypted individual key, and storing the decrypted content key, before said distribution

-20-

00265507

key is updated, thereby making it possible to decrypt said content after said distribution key is updated.

149.   (Currently Amended) An information distribution method for sending content data encrypted with a predetermined content key from an information sending device to an information receiving device, ~~characterized by comprising~~

wherein said method comprises:

a sending step of encrypting said content key with an individual key specific to the information sending device, and sending at least said content key encrypted with said individual key, and an encrypted individual key made by encrypting said individual key with <u>one of a plurality of distribution keys, each distribution key corresponding to a predetermined time period</u>~~an distribution key that is updated in a predetermined cycle, which is supplied from the outside~~, to said information receiving device, by said information sending device; and

a storing step of receiving at least said content key encrypted with said individual key, and said encrypted individual key, and decrypting said individual key with ~~said distribution key given in advance~~<u>one of said plurality of distribution keys</u>, decrypting said content key with the decrypted individuals key, and storing the decrypted content key before said distribution key is updated, thereby making it possible to decrypt said content after said distribution key is updated, by said information receiving device.

150.   (Currently Amended) An information receiving device for receiving content data encrypted with a content key distributed from an information sending device, ~~characterized by~~ <u>said device</u> comprising:

-21-

receiving means for receiving at least said content key encrypted with an individual key, and an encrypted individual key made by encrypting said individual key with <u>one of a plurality of distribution keys, each distribution key corresponding to a predetermined time period</u> a distribution key that is updated in a predetermined cycle, which are sent from said information sending device, before said distribution key is updated; and

controlling means for decrypting said individual key with said distribution key given in advance <u>one of said plurality of distribution keys</u>, decrypting said content key with the decrypted individual key, and storing the decrypted content key before said distribution key is updated, thereby making it possible to decrypt said content after said distribution key is updated.

151.   (Original) The information receiving device according to Claim 150, characterized in that said receiving means receives said content key encrypted wit:, said individual key specific to said information sending device, and said encrypted individual key, before said distribution key is updated.

152.   (Original) The information receiving device according to Claim 151, characterized in that said controlling means encrypts said content key decrypted using said distribution key before said update, with a save key, and stores the same.

153.   (Original) The information receiving device according to Claim 152, characterized in that said controlling means encrypts said content key decrypted using said distribution key before said update, with said save key specific to said information receiving device, and stores the same.

-22-

154.   (Original) The information receiving device according to Claim 153, characterized in that

said receiving means receives said content key encrypted with said individual key and

said encrypted individual key, sent from said information sending device, together with a

signature for send, and

said controlling means verifies said signature and decrypts said individual key with said

distribution key given in advance, decrypts said content key with the decrypted individual key,

and stores the decrypted content key, before said distribution key is updated, if it is confirmed

that said content key encrypted with said individual key, and said encrypted individual key are

not tampered.

155.   (Original) The information receiving device according to Claim 154, characterized in that

said receiving means receives said content key encrypted with said individual key and

said encrypted individual key, sent from said information sending device, together with

signatures added separately to said content key encrypted with said individual key and said

encrypted individual key.

156.   (Original) The information receiving device according to Claim 155, characterized in that

said receiving means receives said content key encrypted with said individual key and

said encrypted individual key, sent from said information sending device, together with a

signature added to both of said content key encrypted with said individual key and said

encrypted individual key.

-23-

00265507

157.   (Currently Amended) An information receiving method for receiving content data

encrypted with a content key distributed from an information sending device, ~~characterized by~~

~~comprising~~ wherein said method comprises:

a receiving step of receiving at least said content key encrypted with an individual key,

and an encrypted individual key made by encrypting said individual key with ~~a~~ one of a plurality

of distribution keys, each distribution key corresponding to a predetermined time period

~~distribution key~~ that is updated in a predetermined cycle, sent from said information sending

device, before said distribution key is updated; and

a storing step of decrypting said individual key with said distribution key given in

advance, decrypting said content key with the decrypted individual key, and storing the

decrypted content key before said distribution key is updated, thereby making it possible to

decrypt said content after said distribution key is updated.

158.   (Original) The information receiving method according to Claim 157, characterized in

that

in said receiving step, said content key encrypted with said individual key specific to said

information sending device, and said encrypted individual key are received before said

distribution key is updated.

159.   (Original) The information receiving method according to Claim 158, characterized in

that

in said storing step, said content key decrypted using said distribution key before said

update is encrypted with a save key and is stored.

-24-

160.   (Original) The information sending method according to Claim 159, characterized in that

in said storing step, said content key decrypted using said distribution key before said

update is encrypted with said save key specific to an information receiving device and is stored.

161.   (Original) The information receiving method according to Claim 160, characterized in that

in said receiving step, said content key encrypted with said individual key and said

encrypted individual key, sent from said information sending device, are received together with a

signature for send, and

in said storing step, said signature is verified, and said individual key is decrypted with

said distribution key given in advance, said content key is decrypted with the decrypted

individual key, and the decrypted content key is stored, before said distribution key is updated, if

it is confirmed that said content key encrypted with said individual key and said encrypted

individual key are not tampered.

162.   (Original) The information receiving method according to Claim 161, characterized in that

in said receiving step, said content key encrypted with said individual key and said

encrypted individual key, sent from said information sending device are received together with

signatures added separately to said content key encrypted with said individual key and said

encrypted individual key.

-25-

163.   (Original) The information receiving method according to Claim 162, characterized in that in said receiving step, said content key encrypted with said individual key and said encrypted individual key, sent from said information sending device, are received together with a signature added to both of said content key encrypted with said individual key and said encrypted individual key.

164.   (Currently Amended) A program storing medium for making an information receiving device run a program, ~~characterized by~~ said program storing medium comprising:

a receiving step of receiving at least a content key encrypted with an individual key, and an encrypted individual key made by encrypting said individual key with a <u>one of a plurality of distribution keys, each distribution key corresponding to a predetermined time period,</u> ~~distribution key~~ that is updated in a predetermined cycle, sent from an information sending device sending content data encrypted with said content key, before said distribution key is updated; and

a storing step of decrypting said individual key with <u>one of said plurality of distribution keys</u> ~~said distribution key given in advance~~, decrypting said content key with the decrypted individual key, and storing the decrypted content key before said distribution key is updated, thereby making it possible to decrypt said content after said distribution key is updated.

165.   (Original) The program storing medium according to Claim 164, characterized in that in said receiving step, said content key encrypted with said individual key specific to said information sending device, and said encrypted individual key are received before said distribution key is updated.

-26-

00265507

166.   (Original) The program storing medium according to Claim 165, characterized in that in said storing step, said content key decrypted using said distribution key before said update is encrypted with. a save key and is stored.

167.   (Original) The program storing medium according to Claim 166, characterized in that in said storing step, said content key decrypted using said distribution key before said update is encrypted with said save key specific to an information receiving device and is stored.

168.   (Original) The program storing medium according to Claim 167, characterized in that

in said receiving step, said content key encrypted with said individual key and said encrypted individual key, sent from said information sending device, are received together with a signature for send, and

in said storing step, said signature is verified, and said individual key is decrypted with said distribution key given in advance, said content key is decrypted with the decrypted individual key, and the decrypted content key is stored before said distribution key is updated, if it is confirmed that said content key encrypted with said individual key and said encrypted individual key are not tampered.

169.   (Original) The program storing medium according to Claim 168, characterized in that in said receiving step, said content key encrypted with said individual key and said encrypted individual key, sent from said information sending device, are received together with signatures

-27-

added separately to said content key encrypted with said individual key and said encrypted individual key.

170. (Original) The program storing medium according to Claim 169, characterized in that in said receiving step, said content key encrypted with said individual key and said encrypted individual key, sent from said information sending device, are received together with a signature added to both of said content key encrypted with said individual key and said encrypted individual key.

171-218. (Canceled)

-28-

00265507